For Official Use Only

When Filled In

C01 PDL Summary Report

PDL:	Lev I/II DOD - Level I and II Certification for DOD sites	**Discrepancy Group:**	PDI-Traditional - Traditional

Screen Sort Order:	CS - 010	**Report Sort Order:**	CS - 010	**PDI Key**	5449
Short Description Identifier:	CS - 010			**Process Status:**	Production

External System ID:	
PDI Short Description:	The COMSEC account is not managed in accordance with NSA or Service Standards.
Default Severity:	Category II
Reference:	NSA Manual 90-2
Default Vulnerability Discussion:	Improper COMSEC account management can result in the loss or compromise of classified cryptologic devices or key.
Default Finding Details:	
Default Recommendation:	Ensure that a person has been identified to be either the COMSEC custodian or Hand Receipt Holder. (NSA Manual 90-2, paragraph 3001) Ensure that COMSEC material is stored in a GSA approved container such as safe, vault, or secure room. (NSA Manual 90-2, paragraphs 6005, and 14002)
Supplemental Information:	Level 1 Certification SIPRNet Compliance Validation

Screen Sort Order:	CS - 040	**Report Sort Order:**	CS - 040	**PDI Key**	5453
Short Description Identifier:	CS - 040			**Process Status:**	Production

External System ID:	
PDI Short Description:	A Protected Distribution System (PDS) is required, however it has not been approved by the cognizant authority, and/or it is not constructed, configured, inspected, monitored and maintained in accordance with established requirements/guidelines.
Default Severity:	Category I
Reference:	NSTISSI 7003
Default Vulnerability Discussion:	A PDS that is not approved or that is not constructed, configured, inspected, monitored and maintained as required could result in the interception of classified information.
Default Finding Details:	
Default Recommendation:	1. Ensure that classified circuits exiting a control space is either encrypted or secured in an approved PDS. 2. If the classified circuits are secured in a PDS, ensure that the PDS is approved by the cognizant authority and constructed, configured, inspected, monitored and maintained as follows: a. The PDS is approved for use by the approving authority. NSTISSI 7003, para 8. b. The PDS terminal equipment is in a controlled area. NSTISSI 7003, Annex B para 1a(1). c. Periodic visual inspections are conducted as required. NSTISSI 7003, Annex B para 1a(6). d. The PDS lines are in full view of personnel conducting required inspections. NSTISSI 7003, Annex B para 1a(2). e. Records of inspection are being maintained. NSTISSI 7003, Annex B para 1a(4).

f. Personnel are aware that the PDS exists; they have been trained to conduct inspections and report any suspicious activity. NSTISSI 7003, Annex B para 1a(3).
g. Hardened carriers will be constructed as follows: NSTISSI 7003, Annex B para 4a.
1. Data cables must be installed in a carrier constructed of electrical metallic tubing (EMT), ferrous conduit or pipe, or rigid-sheet steel ducting, utilizing elbows, couplings, nipples and connectors of the same material.
2. The PDS pull boxes (if used):
(a) The covers are sealed at mating surfaces.
(b) The hinge pins are non-removable.
(c) The box is secured with a GSA approved changeable combination padlock.
3. The PDS connections are permanently sealed surfaces (welding, compression, epoxy, fusion, etc).
4. If the PDS is buried, it is at least 1 meter below the surface (CONUS or US government owned or leased property).
5. Access manholes should be secured with a GSA approved changeable combination lock or a standard locking manhole cover with micro-switch alarms.
6. Suspended systems between buildings should be elevated a minimum of 5 meters above the ground and only used if the property traversed is owned or leased by the US government.
h. Simple carriers will be constructed as follows: NSTISSI 7003, Annex B para 4b.
1. Data cables should be installed in a carrier constructed of any material (wood, PVC, EMT, ferrous conduit.
2. Joints and access points should be secured and controlled by personnel cleared to the highest level of data handled by the PDS.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Checklist

Screen Sort Order:	CS - 050	**Report Sort Order:**	CS - 050	**PDI Key**	5454
Short Description Identifier:	CS - 050			**Process Status:**	Production

External System ID:

PDI Short Description: Protection of controlled unclassified information during transmission is not utilizing DES or another method meeting the requirements of FIPS 140.

Default Severity: Category III

Reference: DODD C-5200.5, para D.1; FIPS 140

Default Vulnerability Discussion: Failure to protect controlled unclassified information can result in its inadvertent release to unauthorized personnel.

Default Finding Details:

Default Recommendation: Ensure controlled unclassified information is properly protected during transmission.

Supplemental Information: Level 1

Screen Sort Order:	IS - 040	**Report Sort Order:**	IS - 040	**PDI Key**	5467
Short Description Identifier:	IS - 040			**Process Status:**	Production

External System ID:

PDI Short Description: Classified documents, media, or equipment are not properly marked with the highest classification of the material/processing and any additional markings/designations as required.

Default Severity: Category II

Reference: DOD 5200.1-R, Chapter 5; DOD 5200.1-PH

Default Vulnerability Discussion: Failure to properly mark classified material could result in the loss or compromise of classified information.

Default Finding Details:

Default Recommendation: Properly mark all classified material, to include documents, media, and equipment. Electronic labeling, designation or marking shall clearly identify all classified material. If physical marking of the medium containing classified information is not possible, then identification of classified information must be accomplished by other means.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order: IS - 050 **Report Sort Order:** IS - 050 **PDI Key** 5468

Short Description Identifier: IS - 050 **Process Status:** Production

External System ID:

PDI Short Description: Classified material and equipment are not stored in accordance with its highest classification level or to the level of classified data being processed.

Default Severity: Category I

Reference: DOD 5200.1-R, para 6-402

Default Vulnerability Discussion: Failure to store classified in an approved container can lead to the loss or compromise of classified or sensitive information.

Default Finding Details:

Default Recommendation: If classified material is to be stored or processed, establish a secure means of storing all classified material. Approved storage may be in a GSA approved safe, vault, or an approved secure room. Ensure storage meets or exceeds requirements for the classification level and type of material stored.

Supplemental Information: SIPRNet Compliance Validation

Screen Sort Order: IS - 060 **Report Sort Order:** IS - 060 **PDI Key** 5469

Short Description Identifier: IS - 060 **Process Status:** Production

External System ID:

PDI Short Description: Personnel who are granted access to classified information do not have a valid Need-to-Know, proper security clearance, and/or have not executed a Non-Disclosure Agreement.

Default Severity: Category I

Reference: DOD 5200.1-R, para 1-101e, para 6-200 and para 9-200b

Default Vulnerability Discussion: Failure to verify clearance, need-to-know, and execute a non-disclosure agreement before granting access to classified can result in unauthorized personnel having access to classified.

Default Finding Details:

Default Recommendation: Prior to receiving access to classified information it must be determined that an individual has met the following requirements:
a. The person has the appropriate clearance and access eligibility.
b. The person has signed an approved non-disclosure agreement.
c. The person has a need-to-know the information.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order: IS - 140 **Report Sort Order:** IS - 140 **PDI Key** 5552

Short Description Identifier: IS - 140 **Process Status:** Production

External System ID:

PDI Short Description: Classified material is not being destroyed in an approved method for level of classification or type of material.

Default Severity: Category II

Reference: DoD 5200.1-R, para 6-701

Default Vulnerability Discussion: Failure to properly destroy classified material can lead to the loss or compromise of classified or sensitive information.

Default Finding Details:

Default Recommendation: Establish procedures for the destruction of classified material using approved methods based on the type of material to be destroyed.
a. Methods and equipment used to routinely destroy paper classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing.
b. Technical guidance concerning appropriate methods, equipment, and standards for the destruction of classified electronic media, processing equipment components, and the like may be obtained by contacting the Directorate for Information Systems Security, National Security Agency, Ft. Meade, MD 20755. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order:	IS - 210	**Report Sort Order:**	IS - 210	**PDI Key**	5483
Short Description Identifier:	IS - 210			**Process Status:**	Production

External System ID:

PDI Short Description: Procedures and policies have not been established to properly protect top-secret material.

Default Severity: Category II

Reference: DISAI 240-110-8 Chapter 7 Section C Paragraph 12

Default Vulnerability Discussion: Failure to establish policies and procedures for the handling of top-secret material can result in the loss or compromise of top-secret material.

Default Finding Details:

Default Recommendation: Ensure procedures and policies have been established to protect top-secret material. This will include:
a. Ensuring a Top Secret Control Officer (TSCO) is appointed in writing and properly trained.
b. An SOP is developed on the handling of top-secret material.
c. Ensure an inventory program is developed, the inventories conducted, and records maintained of the inventories according to standard file management regulations.
d. Top-secret material is reproduced only by TSCOs.

Supplemental Information: DISA Policy Only

Screen Sort Order:	ISS - 010	**Report Sort Order:**	ISS - 010	**PDI Key**	5363
Short Description Identifier:	ISS - 010			**Process Status:**	Production

External System ID:

PDI Short Description: Adequate fire detection and suppression does not exist or is not periodically tested.

Default Severity: Category III

Reference: FIPS PUB 31, NFPA 75, and DODI 8500.2 Enclosure 4 Control Numbers PEFD-2, PEFI-1 and PEFS-2 located in Attachments 1, 2 and 3

Default Vulnerability Discussion: Failure to provide adequate fire detection and suppression could result in the loss of or damage to data, equipment, facilities, or personnel.

Default Finding Details:

Default Recommendation: Ensure adequate fire detection and suppression are available, commensurate with the size of the system. Fire detection and suppression must be periodically tested to ensure effectiveness.

Supplemental Information: Ask if server room has sprinklers or a hand-held fire extinguisher within 50 feet of equipment. Visually inspect area. Ensure fire extinguisher is minimally rated for electrical fires (Class C in the form of carbon dioxide, dry chemical or halon type agents.

Screen Sort Order:	ISS - 020	**Report Sort Order:**	ISS - 020	**PDI Key**	5488
Short Description Identifier:	ISS - 020			**Process Status:**	Production

External System ID:

PDI Short Description: Security Features Users Guides or equivalent (such as Security Standard Operating Procedure) have not been developed or are not available for all systems in the organization.

Default Severity: Category III

Reference: CJCSI 6510.01D Enclosure D para 7a(3), DODI 8500.2 para 5.10.5 and DODI 8500.2 Enclosure 4 Control Number PRRB-1 located in Attachments 1, 2 and 3

Default Vulnerability Discussion: If user guides are not available for the end users, the security features of the systems are weakened and can possibly result in easy compromise by hackers or unauthorized individuals.

Default Finding Details:

Default Recommendation: Ensure user guides are available for all systems and as a minimum the following areas are documented:
a. Handling of suspected system compromise
b. Information Operations Condition (INFOCON) procedures and policies
c. Periods Processing (if applicable)
d. Procedures for eradication after an attack
e. Proper password management
f. Purging of storage media (disks, drives, etc) prior to turn-in or disposal
g. Remote diagnostic and maintenance
h. Turn-in of equipment
i. Use of screensavers/Unattended terminals
j. Virus detection and scanning
k. Warning Banners

Supplemental Information: Ask if an SFUG or Security SOP has been developed and approved. View copy if time permits to ensure required topics are covered.

Screen Sort Order:	ISS - 030	**Report Sort Order:**	ISS - 030	**PDI Key**	5489
Short Description Identifier:	ISS - 030			**Process Status:**	Production

External System ID:

PDI Short Description: There is no configuration management process (which includes the IAO/IAM) to evaluate and approve system changes to software, firmware, and hardware that will affect the security of the system.

Default Severity: Category II

Reference: NIST 800-14, para 3.9, DODD 8500.1 para 4.17; DODI 8500.2 Enclosure 4 Control Number DCPR-1 located in attchments 1, 2 and 3; DODI 8500.2 Enclosure 4 Control Number DCCB-1 located in attchments 1, 2 and 3;CJCSI 6510.01D Enclosure D, para 13.a

Default Vulnerability Discussion: Security vulnerabilities may be introduced when changes take place in the environment that have not been reviewed by the security personnel in conjunction with a configuration control board process.

Default Finding Details:

Default Recommendation: The IAO/IAM is responsible for ensuring that there are no security risks presented by software, firmware, or hardware introduced at the facility. Implement a configuration management process that includes the IAO/IAM.

Supplemental Information: Ask the IAM if a configuration control board (CCB) exists and if security is a participating member of the CCB. If time permits ask to see a copy of the CCB charter or other documentation.

Screen Sort Order:	ISS - 040	**Report Sort Order:**	ISS - 040	**PDI Key**	5490
Short Description Identifier:	ISS - 040			**Process Status:**	Production
External System ID:					

PDI Short Description: Continuity of Operations Plans (COOP) have not been developed and/or tested to ensure system and data availability in the event of any type of failure. COOP is not commensurate with the assigned Mission Assurance Category (MAC) for the system(s).

Default Severity: Category II

Reference: CJCSI 6510.01D Enclosure D, para 10; DODD 8500.1, para 4.7; DODI 8500.2 IA Controls CODP-1, CODP-2 CODP-3; OMB Circular NO. A-130, Appendix III, para A3a2e

Default Vulnerability Discussion: Failure to develop a COOP and test it periodically can result in the partial or total loss of operations and INFOSEC. A contingency plan is necessary to reduce mission impact in the event of system compromise or disaster.

Default Finding Details:

Default Recommendation: COOP/Disaster Recovery/Contingency plan should address the following:
a. The system has a tested contingency plan addressing full system restoration.
b. Identify the use of another system to be used to avoid interruption of important processing, if the system were destroyed, or in need of repair.
c. Backups are made of critical applications on a regular basis, are selectively tested on a regular basis, and are stored off-site, and the security posture of the off-site location is adequate for their storage.
d. A current, tested, system Emergency Action Plan exists, and assigns clear responsibilities for actions to be taken during the emergency situation. These actions are listed in priority order. The Emergency Action plan is tested periodically to test events with less than catastrophic occurrences as well as events with major catastrophic occurrences.
e. A system Backup Plan exists and:
1. Identifies critical and vital files, which must be backed up to include how the media containing those files are to be marked.
2. Identifies essential documentation that must be available in the event the primary processing site is unavailable.
3. Establishes the frequency of backups and rotation schedule of the backup media.
4. Provides for off site storage of the backed up media and essential documentation.
5. Contains information relating to security of the backed up media, to include while being transported to/from the off-site location.
6. Contains information regarding a backup computer facility.
f. A Disaster Recovery Plan exists and:
1. Establishes evaluation criteria for determining the extent of disruption of functions and operations.
2. Identifies backup processing site(s).
3. Covers the safeguarding or destruction of classified or sensitive information in the event that the primary site must be evacuated.
4. Provides detailed plans for the movement of personnel and the backup media/documentation to the backup processing site.
5. Provides guidance for testing the plan.
g. Responsibilities are clearly and unambiguously assigned in the Contingency Plan.
h. The organizations Contingency Plans clearly outlines the amount of downtime that can be tolerated before disaster is declared.
i. The comprehensiveness of the COOP is dependant upon the MAC Level of the system or enclave, MAC I being the highest criticallity.

Supplemental Information: Ask if COOP plan has been: developed, documented, approved, and tested. Was COOP developed commensurate with the assigned MAC Level.

Screen Sort Order:	ISS - 050	**Report Sort Order:**	ISS - 050	**PDI Key**	5491
Short Description Identifier:	ISS - 050			**Process Status:**	Production
External System ID:					

PDI Short Description: A program does not exist to recognize, investigate, and report information systems security incidents to include virus, system penetration, and classified contamination.

Default Severity: Category II

Reference:	CJCSI 6510.01D, Enclosure D, para 20c; CJCSI 6510.01D Enclosure C, para 1c(5); CJCSI 6510.01D Enclosure C, para 7; DODI 8500.2 para 5.8.5, para 5.9.10 and para 5.12.3
Default Vulnerability Discussion:	Failure to recognize, investigate and report information systems security incidents could result in the loss of confidentiality, integrity, and availability of the systems and its data.
Default Finding Details:	
Default Recommendation:	Establish a program to recognize, investigate, and report information systems security incidents.
Supplemental Information:	Ask to see computer security incident handling procedures either in a Security SOP or other document. Review if time permits to ensure completeness.

Screen Sort Order:	ISS - 090	**Report Sort Order:**	ISS - 090	**PDI Key**	5495
Short Description Identifier:	ISS - 090			**Process Status:**	Production
External System ID:					
PDI Short Description:	A System Access Control Form (DD Form 2875 or equivalent) is not being used to define and control individual access.				
Default Severity:	Category II				
Reference:	DODI 8500.2 Enclosure 4 Attachment 4 Control Number IAAC-1; DODI 8500.2 para 5.10.1 and para 5.11.2; CJCSM 6510.01 Appendix A Enclosure A para 8 (draft)				
Default Vulnerability Discussion:	If accurate records of authorized users are not maintained, then unauthorized personnel could have access to the system.				
Default Finding Details:					
Default Recommendation:	Initiate a System Access Control Form for each person who requests logon access to a computer system. The IAO will retain all forms for each person granted access to their systems.				
Supplemental Information:	Ask to review the user registration form being used to document users. If not a DD Form 2875, ensure their form has the same functionality.				

Screen Sort Order:	ISS - 100	**Report Sort Order:**	ISS - 100	**PDI Key**	5494
Short Description Identifier:	ISS - 100			**Process Status:**	Production
External System ID:					
PDI Short Description:	There is no procedure that implements DOD policy to ensure that users, System Administrators and Network Administrators are properly trained and certified.				
Default Severity:	Category II				
Reference:	CJCSI 6510.01D, Enclosure B, para 14				
Default Vulnerability Discussion:	Improperly trained personnel can cause serious system-wide/network-wide problems that render a system/network unstable.				
Default Finding Details:					
Default Recommendation:	Develop a procedure to ensure that all DOD personnel and support contractors are trained and appropriately certified to perform the tasks associated with their responsibilities for safeguarding and operating DOD information systems.				
Supplemental Information:	Ask if System Administrators are at least Level 1 certified. Is the policy requiring certification contained in their Security SOP? Do all users receive initial IA training before being given access to the system?				

Screen Sort Order:	ISS - 110	**Report Sort Order:**	ISS - 110	**PDI Key**	5497
Short Description Identifier:	ISS - 110			**Process Status:**	Production

External System ID:

PDI Short Description: There is not a least privilege policy in effect that ensures the user has access to all of the information to which the user is entitled, but to no more, to include foreign nationals if they are approved for access.

Default Severity: Category II

Reference: DODI 8500.2 Enclosure 4 Control Number ECLP-1 located in Attachments 4, 5 and 6

Default Vulnerability Discussion: Without a least privilege policy a user can gain access to information that he or she is not entitled to and can compromise confidentiality, integrity and availability of the system.

Default Finding Details:

Default Recommendation: Establish a least privilege policy that controls access to systems and services, user data, configuration and management data and install security mechanisms.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order:	ISS - 180	**Report Sort Order:**	ISS - 180	**PDI Key**	5504
Short Description Identifier:	ISS - 180			**Process Status:**	Production

External System ID:

PDI Short Description: A System Security Authorization Agreement (SSAA) and related security documents have not been developed and submitted to the appropriate authority for approval.

Default Severity: Category III

Reference: DOD 8510.1-M, para C2.1.1.5

Default Vulnerability Discussion: Failure to provide the proper documentation can lead to a system connecting without all proper safeguards in place, creating a threat to the networks.

Default Finding Details:

Default Recommendation: Ensure the SSAA and related security documentation are developed in accordance with DITSCAP requirements, properly submitted and approved. A copy of the SSAA and security documentation will be maintained on-site by the organization.

Supplemental Information: Ask to see a copy of the ATO/IATO letter. Is it current? Ask if a full SSAA support the ATO/IATO.

Screen Sort Order:	ISS - 190	**Report Sort Order:**	ISS - 190	**PDI Key**	5505
Short Description Identifier:	ISS - 190			**Process Status:**	Production

External System ID:

PDI Short Description: Procedures are not developed to maintain the accredited baseline including notification to the approving authority in the event of changes to the baseline.

Default Severity: Category III

Reference: CJCSI 6510.01D Enclosure D, para 13a(4)

Default Vulnerability Discussion: Without proper procedures in place for maintaining the accredited baseline, changes could be made which would negate the accreditation of the system and possibly cause a disruption in the systems operation.

Default Finding Details:

Default Recommendation: Establish and maintain a set of procedures to properly maintain the accredited baseline of the system.

Supplemental Information: Level 1 Certification

Screen Sort Order:	ISS - 200	**Report Sort Order:**	ISS - 200	**PDI Key**	5506

Short Description Identifier: ISS - 200

Process Status: Production

External System ID:

PDI Short Description: The command does not have at least an Interim Approval to Connect (IATC) to NIPRNET and must be in compliance with the NIPRNET Connection Approval Process to include a waiver for Internet connectivity, if applicable.

Default Severity: Category III

Reference: CJCSI 6211.02B, Appexdix B to Encl C

Default Vulnerability Discussion: Failure to provide to the current connection documentation can result in a threat to the NIPRNet connected systems.

Default Finding Details:

Default Recommendation: Ensure an IATC is obtained for connection to the NIPRNet by the organization.

Supplemental Information: ATC/IATC may be reviewed ahead of time on the NIPRNET database http://www.nic.mil/dodnic.mil/index_no.html or https://cap.nipr.mil. If not, ask to see at site. Ensure ATC/IATC is current. Check with technical reviewers to ensure there are no back-door connection to the Internet, that are not already covered by a waiver.

Screen Sort Order: ISS - 290 **Report Sort Order:** ISS - 290 **PDI Key** 5515

Short Description Identifier: ISS - 290

Process Status: Production

External System ID:

PDI Short Description: 1. The command has not designated a primary and alternate point of contact responsible for Information Assurance Vulnerability Alert (IAVA).
2. The IAVA POC does not acknowledge receipt of all IAVA notifications within 5 days or report compliance via the appropriate IAVA web site, within 30 days.

Default Severity: Category II

Reference: DEPSECDEF Memo, 30 Dec 99, para 2.a, b, d, 3.a

Default Vulnerability Discussion: The command will not be aware of the latest vulnerabilities and upgrades affecting their systems which could result in the loss or compromise of information.

Default Finding Details:

Default Recommendation: Assign a primary and alternate POC, and ensure compliance in accordance with the DECSECDEF Memo.

Supplemental Information: Ask if the organization receives and applies IAVA notices. Is there an IAVA tracking system? VCTS is only required for DISA and other participating organizations.

Screen Sort Order: ISS - 330 **Report Sort Order:** ISS - 330 **PDI Key** 5564

Short Description Identifier: ISS - 330

Process Status: Production

External System ID:

PDI Short Description: Procedures are not in place to identify access requests by foreign nationals.

Default Severity: Category II

Reference: CJCSI 6510.01D, Enclosure B para 9b and para 9c

Default Vulnerability Discussion: Unauthorized access by foreign nationals to Information Systems can result in, among other things, security incidents, compromise of the system, or the introduction of a virus.

Default Finding Details:

Default Recommendation: Develop written procedures whereby all foreign access requests are documented and permitted only after a thorough review by security personnel.

Supplemental Information: Ask if any foreign nationals have access to the system. Ensure approval has been received to allow access. Access to NIPRNET requires service level approval.

Screen Sort Order: PE - 030 **Report Sort Order:** PE - 030 **PDI Key** 5520

Short Description Identifier: PE - 030 **Process Status:** Production

External System ID:

PDI Short Description: Individuals are not familiar with pertinent security regulations nor are they aware of standards of conduct required of persons holding positions of trust.

Default Severity: Category III

Reference: DOD 5200.2-R, para 9-103 (Internet version para C9.1.4)

Default Vulnerability Discussion: Failure to inform personnel of the expected standards of conduct while holding a position of trust can result in conduct by the individual that will require them being removed from that position.

Default Finding Details:

Default Recommendation: Provide training to all employees on security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. Individuals must be able to recognize and avoid the kind of personal behavior that would result in rendering them ineligible for continued assignment in a position of trust.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order: PE - 040 **Report Sort Order:** PE - 040 **PDI Key** 5521

Short Description Identifier: PE - 040 **Process Status:** Production

External System ID:

PDI Short Description: DOD military, civilian and contractor positions (if required by DD Form 254) have not been designated with position sensitivity based on the required access of their position to classified information or other sensitive duties.

Default Severity: Category II

Reference: DOD 5200.2-R para 3-101 or para 3-400 (Internet version para C3.1.2 or C3.4)

Default Vulnerability Discussion: Failure to designate position sensitivity could result in personnel having access to classified information or other sensitive duties without the required investigative and adjudicative prerequisites.

Default Finding Details:

Default Recommendation: Ensure all DOD military, civilian and contractor positions are designated to reflect clearance requirements and any other sensitive duties. Review all positions for the correct clearance requirement.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order: PE - 050 **Report Sort Order:** PE - 050 **PDI Key** 5522

Short Description Identifier: PE - 050 **Process Status:** Production

External System ID:

PDI Short Description: Validation of security clearance has not been obtained for each individual given access to classified.

Default Severity: Category III

Reference: DOD 5200.2-R, para 7-101 (Internet version para C7.1.1)

Default Vulnerability Discussion: Failure to verify security clearance status could result in an unauthorized person having access to classified information or an authorized person being unable to perform assigned duties.

Default Finding Details:

Default Recommendation: Ensure a security clearance validation is obtained from an approved Personnel Security Roster or Clearance Certificate and posted to each individuals local security file.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order:	PE - 070	**Report Sort Order:**	PE - 070	**PDI Key**	5524
Short Description Identifier:	PE - 070			**Process Status:**	Production

External System ID:

PDI Short Description: DOD military, civilian personnel, and contractor personnel have not been assigned with one of the three IT (ADP) designations based on specific criteria as designated in DOD 5200.2-R, Appendix K (Internet version Appendix 10).

Default Severity: Category II

Reference: DOD 5200.2-R para 3-614 (Internet version para C3.6.15) and Appendix K (Internet version Appendix 10); DODD 8500.1, para 4.8 E2.1.24; CJCSI 6510.01C, Enclosure A, para 2n(5)

Default Vulnerability Discussion: Failure to designate an appropriate IT level could result in an individual having access to an information system without the required investigative and adjudicative prerequisites.

Default Finding Details:

Default Recommendation: Ensure all positions; military, civilian, and contractors, are assigned to one of the three IT levels. Designations should be noted on Position Descriptions for Civilian Employees, JTD for Military Personnel, and in the Statement of Work or Contract for contractors.

Supplemental Information: Ask if an IT (ADP) Designation Program exists. Ask if all positions have been designated. Look at documentation such as DD Forms 2875 or Personnel Security Rosters to check if different IT levels are designated. Ask for proof of IT level of a known SA and confirm if IT I was granted and the individual has an SSBI (or it is in process.)

Screen Sort Order:	PH - 010	**Report Sort Order:**	PH - 010	**PDI Key**	5533
Short Description Identifier:	PH - 010			**Process Status:**	Production

External System ID:

PDI Short Description: A physical security program has not been developed by the command establishing active and passive measures designed to prevent unauthorized access to installations, facilities, personnel, equipment, material, and documents that safeguard them from espionage, sabotage, damage and theft.

Default Severity: Category III

Reference: DODD 5200-8R, Chapter 2, para C2.1.1

Default Vulnerability Discussion: Failure to have a physical security program could result in an increased risk to personnel, equipment, material and documents.

Default Finding Details:

Default Recommendation: Develop a physical security program to provide guidance and the means to counter threats during peacetime, transition to war, and in wartime.

Supplemental Information: SIPRNet Compliance Validation
Level 1 Certification

Screen Sort Order:	PH - 020	**Report Sort Order:**	PH - 020	**PDI Key**	5534
Short Description Identifier:	PH - 020			**Process Status:**	Production

External System ID:

PDI Short Description: A risk analysis has not been conducted and documented for the systems and the facility.

Default Severity: Category III

Reference: DOD 8510.1-M, para C2.2; CJCSI 6510.01D Enclosure D para 17c

Default Vulnerability Discussion: Failure to conduct a risk analysis could result in not implementing an effective countermeasure to a vulnerability or wasting resources on ineffective measures leading to a possible loss of classified, equipment, facilities, or personnel.

Default Finding Details:

Default Recommendation: Prepare a risk analysis for the system and facility. The commander/director will sign the risk analysis, signifying acceptance of any residual risk.

Supplemental Information: Ask if a Risk Analysis has been conducted. It is normally documented in the SSAA. If time permits, ask to see/review it. The RA should be no older than the SSAA but is preferably updated annually.

Screen Sort Order:	PH - 025	**Report Sort Order:**	PH - 025	**PDI Key**	8936
Short Description Identifier:	PH - 025			**Process Status:**	Production

External System ID:

PDI Short Description: Major components of sensitive systems, such as servers, hubs, and switches, allow physical access to personnel without the need-to-know.

Default Severity: Category II

Reference: DODI 8500.2, IA Control PECF-1

Default Vulnerability Discussion: Allowing access to systems processing sensitive information by personnel without the need-to-know could permit loss, destruction of data or equipment or a denial of service. Loss could be accidental damage or intentional theft or sabotage.

Default Finding Details:

Default Recommendation: Ensure all major system assets such as servers, hubs, and switches are protected by at least a key locked room, separately zoned access control rooms, or locked computer cabinets.

Supplemental Information: Physically inspect room that houses the servers. For unclassified systems: is the room locked with a key, swipe card, or cipher lock? Can only the personnel who need access to the system have unescorted access? If the room is shared with other employees is the server located in a locked cabinet?

Screen Sort Order:	PH - 050	**Report Sort Order:**	PH - 050	**PDI Key**	5537
Short Description Identifier:	PH - 050			**Process Status:**	Production

External System ID:

PDI Short Description: A program has not been established to identify and control visitors in controlled areas.

Default Severity: Category II

Reference: DODI 8500.2 Enclosure 4 Control Number PEVC-1 located in Attachments 4 and 5

Default Vulnerability Discussion: Failure to identify and control visitors could result in unauthorized personnel gaining access to the facility with the intent to compromise classified information, steal equipment, or damage equipment or the facility.

Default Finding Details:

Default Recommendation: Establish a program to control visitors. Program will include verification of clearance/investigation status, personal identification of visitor, registering of visitors, proper badging, and escorts, if required.

Supplemental Information: SIPRNet Compliance Validation

Screen Sort Order:	PH - 060	**Report Sort Order:**	PH - 060	**PDI Key**	5538
Short Description Identifier:	PH - 060			**Process Status:**	Production

External System ID:

PDI Short Description: Control of sensitive items is not maintained. This includes keys, badges, smart cards.

Default Severity: Category II

Reference: DOD 5100.8-R, para C1.3.3 and Best Practices

Default Vulnerability Discussion: Lack of an adequate key/access device control could result in unauthorized personnel gaining access to the facility or systems with the intent to compromise classified information, steal equipment, or damage equipment or the facility.

Default Finding Details:

Default Recommendation: Establish a control program for all sensitive items. Store master and extra keys or devices in a locked container, have all personnel sign for sensitive items and establish procedures to maintain logs.

Supplemental Information:

Screen Sort Order:	SM - 010	**Report Sort Order:**	SM - 010	**PDI Key**	5546
Short Description Identifier:	SM - 010			**Process Status:**	Production

External System ID:

PDI Short Description: 1. A properly trained security staff, allowing for separation of duties with each individual assigned to specific duties, has not been appointed in writing.
2. Information Assurance Managers (IAMs) and Information Assurance Officers (IAOs) must be US citizens.

Default Severity: Category III

Reference: DoD 5200.1-R, para 1-201c; DODI 8500.2 para 5.8.2 and 5.9.5; CJCSI 6510.01D Enclosure B para 14b; CJCSI 6510.01D Enclosure D para 3b and para 3c

Default Vulnerability Discussion: Failure to appoint security personnel could result in a weak security program.

Default Finding Details:

Default Recommendation: 1. The position structure of the security staff should allow for separation of duties by filling the following positions as a minimum.
a. An IAM is appointed to oversee the Information System Security Program.
b. An IAO is appointed for each system or type of system in the organization.
c. A Security Manager (SM) is appointed to oversee the Traditional Security Program.
2. All security professionals assigned to the security staff should have received the appropriate training.
3. All appointments should be in writing and signed by the current commander/director.
4. Ensure the IAM is a US citizen.
5. If IAO is newly appointed, they must be a US citizen. If the IAO was appointed prior to Feb 03 they must be under the supervision of an IAM who is a US citizen and be approved in writing by the DAA.

Supplemental Information: Ask for copies of the appointment order for the IAM, IAO, and if possible the SM. Ask if these employees have been trained and/or certified if applicable.

Screen Sort Order:	SM - 020	**Report Sort Order:**	SM - 020	**PDI Key**	5547
Short Description Identifier:	SM - 020			**Process Status:**	Production

External System ID:

PDI Short Description: A program does not exist to ensure personnel out process through the security section.

Default Severity: Category III

Reference: DOD 5200.1-R, para 9-500

Default Vulnerability Discussion: Failure to properly out process through the security section allows the possibility of unauthorized access to the facility and/or the systems.

Default Finding Details:

Default Recommendation: Ensure that all personnel departing the organization out process through the security section, to include turning in of all access badges, classified or sensitive information and signing of SF 312 acknowledging debriefing.

Supplemental Information: Level 1 Certification

Screen Sort Order:	SM - 030	**Report Sort Order:**	SM - 030	**PDI Key**	5548
Short Description Identifier:	SM - 030			**Process Status:**	Production

External System ID:

PDI Short Description: Standard Operating Procedures (SOPs) have not been developed detailing all security procedures that are specific to the organization.

Default Severity: Category III

Reference: DoD 5200.1-R, para 1-202e and DoD 5220.22-R, para 1-107

Default Vulnerability Discussion: Failure to have documented procedures in an SOP could result in a security incident due to lack of knowledge by personnel assigned to the organization.

Default Finding Details:

Default Recommendation: Develop a SOP that as a minimum covers the following items:
a. Access Control
b. Classified Handling
c. Computer Security
d. COTS Prohibition
e. Data Sharing
f. Derogatory Information Reporting
g. Emergency Actions
h. End Of Day Procedures
i. Foreign National Access to AIS
j. Foreign Travel
k. Fraud Waste and Abuse
l. Handling of incoming mail/packages
m. Key Control
n. Personnel Security
o. Security Awareness training
p. Security Incident and Reporting

Supplemental Information: SIPRNet Compliance Validation

Screen Sort Order:	SM - 050	**Report Sort Order:**	SM - 050	**PDI Key**	5550
Short Description Identifier:	SM - 050			**Process Status:**	Production

External System ID:

PDI Short Description: Personnel do not receive initial indoctrination and annual training thereafter on the national security implications of their duties and individual responsibilities.

Default Severity: Category III

Reference: DoDD 5200.1-R, para 9-600

Default Vulnerability Discussion: Failure to provide security training results in a weak security program and could lead to the loss or compromise of classified or sensitive information.

Default Finding Details:

Default Recommendation: 1. Provide initial training that covers all areas of security.
2. Establish an annual training plan that covers the following areas as a minimum:
a. Classified Handling
b. Communications Security
c. Computer Security
d. Counter-intelligence

e. Courier briefing (if applicable)
f. Reporting of derogatory information
g. Reporting of Security Incidents
h. Security of Laptop computers when traveling
i. Special access programs, NATO, COSMIC TS, etc (if applicable)
j. Use of personal computers for conducting official business
3. Ensure all training is documented and a copy is maintained to validate that the training has been conducted.

Supplemental Information: Ensure all uses receive initial IA training before being given an account on the system. Ask if annual/periodic refresher training is provided.

Screen Sort Order:	TM - 010	**Report Sort Order:**	TM - 010	**PDI Key**	5543
Short Description Identifier:	TM - 010			**Process Status:**	Production
External System ID:					
PDI Short Description:	TEMPEST countermeasures were not considered prior to establishing a classified work area.				
Default Severity:	Category III				
Reference:	DODD C-5200.19				
Default Vulnerability Discussion:	Failure to implement required TEMPEST countermeasures could leave the system(s) vulnerable to a TEMPEST attack.				
Default Finding Details:					
Default Recommendation:	Consider Tempest countermeasures prior to establishing a classified work area.				
Supplemental Information:	Level 1 Certification				

35 PDI(s) displayed.